What is claimed is:

1. A method of providing cross-domain authentication in a computing environment, comprising steps of:

providing security credentials of an entity to an initial point of contact in the computing environment;

passing the provided credentials from the initial point of contact to a trust proxy;

authenticating the passed credentials with an authentication service in a local security domain of the trust proxy; and

using the authentication performed by the local authentication service to seamlessly authenticate the entity to one or more selected remote security domains.

2. The method according to Claim 1, when the using step further comprises the steps of:

consulting policy information to determine which of a plurality of remote security domains should be selected to receive information from the local authentication service; and

passing the information from the local authentication service to each of the determined remote security domains.

3. The method according to Claim 1, wherein the using step enables remote services in the selected remote security domains to be accessed by the entity without requiring the entity to provide its security credentials for those remote services.

4. The method according to Claim 3, wherein a credential mapping operation is performed to

map the provided security credentials to the entity's security credentials for each remote service.

5. The method according to Claim 1, wherein the entity is an end user.

6. The method according to Claim 1, wherein the initial point of contact is a portal interface.

7. The method according to Claim 1, wherein the passing step is performed by a proxy of the initial point of contact.

8. The method according to Claim 7, wherein the proxy of the initial point of contact performs a protocol conversion, when passing the provided credentials, from a first protocol used in the providing step to a second protocol used by the trust proxy.

9. The method according to Claim 8, wherein the first protocol is Hypertext Transfer Protocol ("HTTP") or a security-enhanced version thereof.

10. The method according to Claim 8, wherein the second protocol is Simple Object Access Protocol ("SOAP").

11. The method according to Claim 1, wherein the initial point of contact provides an aggregation of a plurality of Web services.

12. The method according to Claim 1, wherein the using step further comprises the steps of:

forwarding a security token from the local authentication service to a remote trust proxy in each of the selected remote security domains; and

using the forwarded security token, at each of the remote trust proxies, to authenticate the entity with an authentication service in the remote security domain.

13. The method according to Claim 12, wherein results of the authentication by the authentication service in the local security domain and results of each authentication by the authentication services in each selected remote security domain are returned to the initial point of contact.

14. The method according to Claim 13, further comprising the step of determining, by the initial point of contact, which services and/or views thereof can be provided to the entity based on the returned results.

15. The method according to Claim 1, wherein the entity has security credentials, in at least one of the selected remote security domains, that differ from the provided security credentials, and wherein the using step transparently maps the provided security credentials to the different security credentials.

16. A system for enabling an entity to have seamless access to a plurality of aggregated services which have different identity requirements, comprising:

means for initially authenticating the entity, by a first authentication component, using an identity provided by the entity;

means for mapping the provided identification to the differing identity requirements of at least one service to be aggregated, thereby establishing mapped identity requirements for each of the at least one services;

means for subsequently authenticating the entity, by an authentication component associated with each of the at least one services, using the mapped identity requirements; and

means for aggregating each of the at least one services and a service associated with the initial authentication component, if the authentications thereof are successful, into an aggregated result.

17. The system according to Claim 16, wherein the aggregated result is an aggregated view.

18. The system according to Claim 16, wherein the entity is a programmatic entity.

19. A computer program product for providing federated identity management within a distributed content aggregation framework, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for providing, to the content aggregation framework by a using entity, initial identity information;

computer-readable program code means for authenticating the initial identity information by a first authentication service in a first security domain;

computer-readable program code means for conveying results of the authentication by the first authentication service to one or more selected other authentication services associated with one or more other security domains; and

computer-readable program code means for using the conveyed results to authenticate the using entity to each of the selected other authentication services, without requiring the using entity to provide additional identity information.

20. The computer program product according to Claim 19, wherein the initial identity information is a name and password associated with the using entity.